EXHIBIT I

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation,	)	
Plaintiff and Counterclaim-Defendant,	)	
v.	)	C. A. No.: 04-1199 (SLR)
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware Corporation,	)	
Defendants and Counterclaim-Plaintiffs.	)	

ISS-GA'S SECOND SET OF INTERROGATORIES (NOS. 19-20)

Pursuant to Rule 33 of the Federal Rules of Civil Procedure, defendant and counterclaim-plaintiff Internet Security Systems, Inc., a Georgia corporation ("ISS-GA") directs the following Interrogatories to plaintiff and counterclaim-defendant SRI International, Inc. ("SRI").

In accordance with Fed. R. Civ. P. 33, each Interrogatory herein is to be answered fully and in writing under oath within thirty (30) days of service of these Interrogatories. In answering these Interrogatories, SRI is requested to give full and complete answers based on personal knowledge, as well as the knowledge of any agents, employees, investigators, attorneys, or other persons who may have obtained information on SRI's behalf.

DEFINITIONS AND INSTRUCTIONS

ISS-GA hereby incorporates by reference the Definitions and Instructions from ISS-GA's First Set Of Requests For The Production Of Documents And Things (Nos. 1-92).

INTERROGATORIES

INTERROGATORY NO. 8:

State, in as much detail as possible, SRI's contentions as to why each ground presented in ISS's Supplemental Response To Interrogatry No. 6 does not render the claims of the patents-in-suit invalid, including without limitation, an identification of each element SRI contends is not present in each of the invalidity charts attached as Exhibits 1-23 to ISS's Supplemental Response To Interrogatry No. 6 and all facts supporting or negating SRI's contentions.

INTERROGATORY NO. 9:

State, in as much detail as possible, SRI's contentions as to why the facts disclosed in ISS's Supplemental Response to SRI'S Interrogatory No. 11 and in the Answers of ISS-GA and ISS-DE do not render the patents-in-suit unenforceable by SRI's inequitable conduct. Your answer should include: (a) a statement as to whether or not you contend that the inventors and/or their agents made each identified misrepresentation or omission of fact; (b) for each misrepresentation or omission of fact, a statement as to whether or not you contend that the inventors and/or their agents acted with intent; and

(c) for each publication identified, a detailed explanation of why the publication is not material, or an admission that the publication is material.

Dated: November 15, 2005

Respectfully submitted,

POTTER ANDERSON & CORROON LLP

Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree Street
Atlanta, GA 30303
Tel: (404) 572-4600

Theresa A. Moehlman
Jeffrey D. Blake
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.,
A Georgia Corporation

EXHIBIT J

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants.	Case No. 04-1199-SLR

SRI INTERNATIONAL, INC.'S RESPONSES TO DEFENDANT ISS-GA'S SECOND SET OF INTERROGATORIES [NOS. 19-20] AND SRI'S THIRD SUPPLEMENTAL RESPONSE TO ISS-GA'S INTERROGATORY NO. 17

Pursuant to Federal Rules of Civil Procedure 26 and 33, Plaintiff SRI International, Inc. ("SRI") responds to Defendant Internet Security Systems, Inc.'s, a Georgia corporation, ("ISS-GA") Second Set of Interrogatories as follows:

GENERAL OBJECTIONS

1. SRI objects to the Interrogatories to the extent they seek information protected by the attorney-client privilege, work product doctrine, and/or any other applicable privilege or immunity.

2. SRI objects to the Interrogatories to the extent they seek information that Plaintiff is under an obligation to third parties not to disclose.

3. SRI objects to the Interrogatories to the extent that they seek information that is a matter of public record or that is otherwise equally available to or already in the possession of ISS-GA.

4. SRI objects to the Interrogatories to the extent they seek information not in Plaintiff's possession, custody or control.

5. SRI objects to the Interrogatories to the extent they seek information not relevant to the claims or defenses of any party and not reasonably calculated to lead to the discovery of admissible evidence.

6. SRI objects to the Interrogatories to the extent they are vague, ambiguous, indefinite, overbroad, unduly burdensome, duplicative, cumulative, unlimited in time or scope, unintelligible or otherwise unclear as to the information sought.

7. SRI incorporates herein its objections to the Definitions and Instructions set forth in SRI's responses to ISS-GA's First Set of Requests for the Production of Documents and Things.

8. SRI's investigation, discovery and analysis are ongoing. SRI reserves the right to modify and/or supplement these Interrogatories as additional information becomes available.

9. SRI objects to the Interrogatories to the extent each interrogatory includes subparts that should be propounded, numbered or counted as another interrogatory in accordance with Rule 33.

10. SRI objects to the Interrogatories to the extent they call for a legal opinion or conclusion.

11. SRI objects to the Definitions, Instructions, and Interrogatories to the extent they seek information or the identification of documents not within SRI's possession, custody or control, or refer to persons, entities, or events not known to SRI, on the grounds that such Definitions, Instructions, and Interrogatories: (1) seek to require more of SRI than any obligation imposed by law; (2) subject SRI to unreasonable and undue burden and expense, and; (3) seek to impose upon SRI an obligation to investigate or discover information or materials from third parties or sources which are equally accessible to ISS-GA.

12. SRI incorporates by reference the general objections set forth above into the specific objections and responses set forth below. SRI may repeat a general objection

for emphasis or some other reason. The failure to repeat any general objection does not waive any general objection to the interrogatory. Moreover, SRI does not waive its right to amend its objections.

RESPONSES

INTERROGATORY NO. 17:

Identify each limitation of each claim of each patent-in-suit that SRI contends is not disclosed in the article "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," authored by Phillip A. Porras and Peter G. Neumann, 20th NISSC, October 9, 1997.

RESPONSE TO INTERROGATORY NO. 17 (AUGUST 1, 2005):

SRI objects to this request in that it prematurely seeks SRI's contentions and expert testimony. SRI will abide by the procedural schedule the Court has set forth in this litigation to fully respond to this interrogatory. Subject to the foregoing objection and the General Objections, which are incorporated by reference, SRI states that no claim limitation of either the '615 or '203 patent is disclosed in the article "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," authored by Phillip A. Porras and Peter G. Neumann, 20th NISSC, October 9, 1997, because the article is merely an abstract discussion of ideas.

SRI further states that its investigation is ongoing and that it reserves the right to supplement its response to this interrogatory as appropriate.

AMENDED RESPONSE TO INTERROGATORY NO. 17 (SEPTEMBER 28, 2005):

SRI objects to this request in that it prematurely seeks SRI's contentions and expert testimony. To the extent that ISS provides SRI with contentions regarding any assertion that ISS has about the invalidity of the patents-in-suit in light of the article "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," authored by Phillip A. Porras and Peter G. Neumann, 20th NISSC, October 9, 1997, SRI will respond according to the procedural schedule the Court has set forth in this litigation.

Subject to the foregoing objection and the General Objections, which are incorporated by reference, SRI states that the claimed inventions of the patents-in-suit are not disclosed in the article "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," authored by Phillip A. Porras and Peter G. Neumann, 20th NISSC, October 9, 1997.

SRI further states that its investigation is ongoing and that it reserves the right to supplement its response to this interrogatory as appropriate.

THIRD SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 17 (DECEMBER 15, 2005):

SRI incorporates by reference its previous responses to Interrogatory No. 17 and its discussion in Section 1 of its response to Interrogatory No. 19 of "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," authored by Phillip A. Porras and Peter G. Neumann, 20th NISSC, October 9, 1997.

INTERROGATORY NO. 8 (SIC - 19):

State, in as much detail as possible, SRI's contentions as to why each ground presented in ISS's Supplemental Response To Interrogatory No. 6 does not render the claims of the patents-in-suit invalid, including without limitation, an identification of each element SRI contends is not present in each of the invalidity charts attached as Exhibits 1-23 to ISS's Supplemental Responses to Interrogatory No. 6 and all facts supporting or negating SRI's contentions.

RESPONSE TO INTERROGATORY NO. 8 (SIC - 19):

SRI objects to this interrogatory as premature. Claim construction has not yet occurred in this matter. SRI objects to this interrogatory as seeking information protected from disclosure by the attorney-client privilege and/or attorney work product doctrines. Discovery and analysis in this case are ongoing. ISS's prior art references fail to disclose or suggest claim limitations of the patents-in-suit for at least the reasons set forth below –

there may be other reasons as well. Any response by SRI is preliminary and SRI reserves the right to supplement its response as discovery and analysis proceed.

Without waiving any specific and any applicable general objection, SRI responds as follows:

As an overview, the patents-in-suit are distinguishable over the prior art for at least three main reasons. First, the prior art fails to disclose, enable or suggest a scalable, hierarchical intrusion detection architecture like the one claimed by the patents-in-suit. Second, the art fails to disclose, enable or suggest network monitoring apparatus or methods that analyze and rely on the specific types of network traffic that the inventors of the patents-in-suit discovered are particularly useful in detecting suspicious network activity in an efficient and practically realizable manner. Finally, with regard to the '338 patent, none of the art discloses, enables or suggests building a long-term and short-term statistical profile of network traffic based on the measures recited in the claims and comparing the long-term to the short-term statistical profile to detect suspicious network activity.

Moreover, these claimed features, as well as others, are not disclosed or rendered obvious by any of the asserted combinations of the prior art. Furthermore, there are objective indicia of non-obviousness, including, without limitation: commercial success of the Accused Products; praise in the marketplace (e.g., DARPA); long-felt need; and failure of others. The fact that many other research groups were attempting to create a practical solution to the problem of network intrusion detection, but that none were successful before SRI's inventions (See discussion below) is strong evidence of non-obviousness.

1. EMERALD 1997

The EMERALD 1997 reference was cited to the PTO during prosecution of the '338 patent and hence was considered during prosecution of all of the patents-in-suit.

(See IDS dated July 17, 1999.) As the Patent Office Examiner initialed the IDS listing the EMERALD 1997 reference, he is presumed to have considered this reference and his decision to issue the patents over this reference is presumed correct.

Defendants' citations to the EMERALD 1997 reference do not contain any teachings regarding the specific types of network traffic to monitor as recited in the following independent claims: claim 1 of the '338 patent; claims 1 and 12 of the '203 patent, and claims 1 and 13 of the '615 patent, nor is there any mention of volume related measure as recited in those claims. Further, there is no teaching in the asserted citations of long-term and short-term profiles and the comparison thereof as recited in independent claims 1, 21 and 24 and 25 of the '338 patent.

Further, because Defendants' citations do not disclose the specific type of network traffic to monitor, the EMERALD 1997 reference does not anticipate dependent claims 2-10 and 22 of the '338 patent. Further, because the citations do not disclose long-term and short-term profiles and comparisons thereof, the EMERALD 1997 reference does not anticipate dependent claims 11-17 and 23 of the '338 patent.

Further, the EMERALD 1997 reference does not provide an enabling disclosure of a statistical detection method for detecting suspicious network activity based on analysis of network traffic data as recited in independent claims 1 and 14 of the '212 patent.

Because the asserted citations of the EMERALD 1997 reference do not disclose any of the independent claims of the patents-in-suit, the EMERALD 1997 reference cannot anticipate any of the other asserted dependent claims not specifically addressed above.

2. CMAD

The CMAD paper is not an enabling disclosure of a system. This two page document describes a plan for what SRI intended to build, and is consistently expressed

in the future tense. It is a subset of EMERALD 1997, and therefore cumulative of what was cited to the patent office and considered during the prosecution of the patents-in-suit. Further, as it is cumulative of the EMERALD 1997 reference, it does not disclose or render obvious any of the claims of the patents-in-suit for at least the same reasons presented above in the discussion of the EMERALD 1997 paper. Nor does the combination of CMAD with either EMERALD 1997 or the "Network NIDES" reference render any of the claims obvious because, even if motivated, the combination lacks and/or fails to enable many of the limitations of the claims as discussed with regard to those references.

3. CONCEPTUAL OVERVIEW

The Conceptual Overview is simply a broad description that is cumulative of the EMERALD 1997 paper. It is far from an enabling disclosure of anything. The Conceptual Overview is at best cumulative of the EMERALD 1997 paper and therefore does not disclose or render obvious any of the claims of the patents-in-suit for at least the same reasons presented above in the discussion of the EMERALD 1997 paper. Nor does the combination of this reference with either EMERALD 1997 or the "Network NIDES" reference render any of the claims obvious because, even if motivated, the combination lacks and/or fails to enable many of the limitations of the claims as discussed with regard to those references.

Additionally, there is no discussion in Conceptual Overview of network-entity deployment as required by independent claims 1, 21 and 24 of the '338 patent.

4. CONCEPTUAL DESIGN

The Conceptual Design document is not prior art as it was never published and was maintained as a confidential, SRI internal document. In fact, this document was never even completed.

Further, the document does not indicate its availability on the Internet simply by the inclusion of a URL on the front page. The mere use of a URL on a document is not indicative of availability of the document at that URL. The Defendants have provided no proof of this document's publication on the Internet. Further, SRI is unaware of any evidence that this document was ever made available to the public, on the Internet or otherwise. Accordingly, the reference itself cannot be relied upon to anticipate any of the claims nor can it be combined with any other reference to form the basis of an obviousness contention.

5. LIVE TRAFFIC ANALYSIS

This publication is not prior art. The priority date of all of the patents-in-suit is November 9, 1998. The earliest date alleged for availability of this publication is November 10, 1997, less than one year before the filing date. Further, this paper is incorporated by reference into the specification of the patents-in-suit.

6. NETWORK NIDES

The reference incorrectly styled "Network NIDES" is not an enabling disclosure for any of the subject matter claimed in any of the patents-in-suit. The majority of the document describes how NIDES analyzes host audit records. The description of "Network NIDES" is in a chapter entitled "Future Directions." No product with that name was ever developed by SRI. The cited reference does not enable applying intrusion detection to a network as required by all claims of the patents-in-suit. In fact, the reference itself establishes that it is not enabling: "*Part of this process [the process of applying NIDES to a network] would entail substantial filtering of the network data prior to conversion to NIDES audit records.*" This identifies an important problem in monitoring network traffic – the vast volume of traffic and the need to develop a system for monitoring it.

Further, the reference in the NIDES paper to monitoring "network connections" simply teaches the monitoring of a (converted) log file – it does not teach monitoring network traffic. Further, the NIDES reference does not teach the type of network traffic data to analyze as recited in independent claims 1 and 12 of the '203 patent, claims 1 and 13 of the '615 patent and claim 1-10 and 22 of the '338 patent.

7. JI-NAO

The Defendants have not shown that the Jou reference ("the Ji-Nao reference") anticipates any claim of any of the patents-in-suit.

As an initial matter, there is no indication that the Ji-Nao reference is prior art. ISS27334; SYM_P_0070541 indicates that it was submitted to DARPA in April of 1997 but Defendants have not provided any documents showing that Ji-Nao was made public prior to November 9, 1997.

The '338 Patent

The Defendants have not shown that the Ji-Nao reference anticipates any of the independent claims of the '338 patent. For example, the Ji-Nao reference citations provided by Defendants are silent on the types of measures of network packets used, referring generally to the "names of the packet types." ISS27356; SYM_P_0070564. This is not even an enabling disclosure for what it expressly recites nor does it teach or suggest the specific types of measurements recited in the claims.

Moreover, the dependent claims of the '338 patent include numerous limitations not disclosed or suggested by Defendants' Ji-Nao citations. For example, there is no indication that the system of the Ji-Nao reference monitors network packet data transfer commands, network packet data transfer volume, connection requests, connection denials, correlation of connection requests with denials, network packet data transfer errors, or error codes as required by claims 2-8 and 10. There is no disclosure or

suggestion of transmitting an event record to a network monitor as required by claim 12. Rather, the Ji-Nao reference citations relied upon by Defendants only disclose local detection subsystems transmitting reports to a remote management subsystem, which only has the ability to probe the status of and issue commands to local detection subsystems. ISS27340; SYM_P_0070548. Additionally, there is no disclosure or suggestion of transmitting reports to hierarchically higher network monitors that do correlation as required by claims 13-15. Indeed, the Ji-Nao reference explicitly states that a three level hierarchy is beyond the scope of the reference. ISS27340; SYM_P_0070548. There is no disclosure or suggestion of altering analysis of network packets or severing a communication channel as required by claims 16 and 17 respectively. Finally, the Ji-Nao reference refers to an analysis of ATM cells rather than TCP/IP packets as required by claim 18.

The '203 and '615 Patents

The Defendants have not shown that the Ji-Nao reference anticipates any of the independent claims of the '203 or '615 patents. The Ji-Nao reference is silent on the types of network traffic analyzed by the Ji-Nao system, referring generally to the "names of the packet types." ISS27356; SYM_P_0070564. This is not an enabling disclosure of any kind of network monitoring. Accordingly, Ji-Nao does not anticipate the independent claims of the '203 and '615 patents. Moreover, the Ji-Nao reference does not disclose automatically receiving and integrating reports as required by the independent claims of the '203 and '615 patents. Rather, the Ji-Nao reference refers only to a local detection subsystem and a remote management unit. ISS27340 SYM_P_0070548; . The remote management unit only probes the status of and issues commands to the local detection subsystems. Id.

The '203 and '615 patents include dependent claims that are further distinguishable over the Ji-Nao reference. For example, there is no reference in Ji-Nao to

providing an API for the incorporation of third party tools as required by claims 4 and 15 of the '203 patent and claims 4, 16, of the '615 patent. Ji-Nao does not refer to placing monitors among multiple domains in an enterprise network such as is required by claims 9-10 and 20-21 of the '203 patent and claims 9-10 of the '615 patent. Indeed, the Ji-Nao reference appears to explicitly teach away from this. See, ISS27340; SYM_P_0070548. Additionally, the Ji-Nao reference refers to an ATM network rather than a TCP/IP network, which is required by claims 7 and 18 of the '203 patent and claims 5 and 17 of the '615 patent.

The '212 Patent

The Defendants have not shown that the Ji-Nao reference anticipates any of the independent claims of the '212 patent. For example, the Ji-Nao reference does not disclose automatically receiving and integrating reports as required by the independent claims of the '212 patent. Rather, the Ji-Nao reference refers only to a local detection subsystem and a remote management unit. ISS27340. The remote management unit only probes the status of and issues commands to the local detection subsystems. Id.

The '212 patent includes dependent claims that are further distinguishable over the Ji-Nao reference. For example, Ji-Nao does not refer to placing monitors among multiple domains in an enterprise network as recited in claims 11-12 and 22-23, and indeed, appears to explicitly teach away from this. See, ISS27340; SYM_P_0070548. Additionally, the Ji-Nao reference refers to an ATM network rather than a TCP/IP network, which is required by claims 7 and 18.

The '212 Patent

The Defendants have not shown that the Ji-Nao reference anticipates any of the independent claims of the '212 patent. For example, the Ji-Nao reference does not disclose automatically receiving and integrating reports as required by the independent

claims of the '212 patent. Rather, the Ji-Nao reference refers only to a local detection subsystem and a remote management unit. ISS27340; SYM_P_0070548. The remote management unit only probes the status of and issues commands to the local detection subsystems. Id.

The '212 patent includes dependent claims that are further distinguishable over the Ji-Nao reference. For example, Ji-Nao does not refer to placing monitors among multiple domains in an enterprise network as recited in claims 11-12 and 22-23, and indeed, appears to explicitly teach away from this. See, ISS27340; SYM_P_0070548. Additionally, the Ji-Nao reference refers to an ATM network rather than a TCP/IP network, which is required by claims 7 and 18.

8. NSM

Defendants have only asserted "A Network Security Monitor" reference ("NSM reference") as relevant to the asserted claims of the '338 patent. Defendants, however, have not shown that the NSM reference anticipates any claim of the '338 patent. The NSM reference refers generally to a system deployed on a single LAN that purports to detect unusual traffic on the basis of signature analysis and a comparison of "normal" traffic with monitored traffic. See, ISS04153; SYM_P_0068978, bottom of second column. As an initial matter, it is important to note that the system described in the NSM reference is not hierarchical nor scalable like the EMERALD system described in the '338 patent. ISS04149; SYM_P_0068974. ("Distributed monitoring of wide area networks will be considerably more complex, and will taken up after our LAN monitoring problems have been properly tackled.") Moreover, the claims of the '338 patent include numerous limitations that are neither disclosed nor suggested by the NSM reference.

With regard to the claims 1, 21 and 24, the NSM reference indicates that it builds a mask or matrix of normal network traffic and detects anything outside of the normal

pattern. See, ISS04152; SYM_P_0068977, second full paragraph. The NSM reference however provides no details as to how the matrix of normal behavior is constructed and nothing in the citations asserted by Defendants teaches or suggests that this matrix is a long-term statistical profile as recited in the claims. The NSM reference cites to IDES and the "Denning model," but the procedure by which the matrix of normal behavior is constructed is not disclosed on the face of the NSM reference. Moreover, there is no disclosure or suggestion of building a short-term statistical profile. Instead, the NSM reference discloses comparing snapshots of the current network traffic with the profile of normal traffic every five minutes. See, ISS04153; SYM_P_0068978 first full paragraph. Comparing instantaneous snapshots of network traffic with the matrix of normal network traffic is not comparing a long-term and a short-term statistical profile as required by the independent claims. Moreover, it appears that the NSM reference merely counts packets and looks for abnormal packet count. A packet count is not a "short-term statistical profile" or a "long-term statistical profile."

The dependent claims of the '338 patent include numerous limitations not disclosed or suggested by the NSM reference. For example, there is no indication that the system of the NSM reference monitors network packet data transfer commands, network packet data transfer volume, connection requests, connection denials, correlation of connection requests with denials, network packet data transfer errors, or error codes as required by claims 2-8 and 10. Moreover there is no enabling disclosure in the NSM reference of responding as a result of detecting suspicious network activity as required by claims 11-12. Rather, the NSM reference includes a vague reference to reporting problems to a security officer and explicitly states that there is no NSM user interface for handling reports. See, ISS04153; SYM_P_0068978, second full paragraph. Additionally, there is no disclosure or suggestion of transmitting reports to hierarchically higher network monitors that do correlation as required by claims 13-15. Indeed, the NSM reference explicitly teaches away from using hierarchy, calling such a system

"considerably more complex." ISS04149; SYM_P_0068978, first full paragraph. There is no disclosure or suggestion of altering analysis of network packets or severing a communication channel as required by claims 16 and 17 respectively. The NSM reference's system does not deploy monitors at a gateway, router or proxy server as required by claim 19.

9. DIDS

The Defendants have not shown that the DIDS articles anticipate any claim of the patents-in-suit for at least the following reasons:

Documents relating to DIDS, including, Snapp, "Signature Analysis and Communications Issues in a Distributed Intrusion Detection System," Thesis 1991 and Snapp et al., "DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype, "Computer Security Laboratory, Division of Computer Science, Univ. of California, Davis, Davis, CA, (hereinafter, "DIDS October 1991") were cited to the Examiner during prosecution of the patents-in-suit. As the Examiner initialed the IDS listing these references he is presumed to have considered them in his decision to issue the patents. Further, his decision to allow the patents over these references is presumed correct. Steven Snapp et al., "Intrusion Detection Systems (IDS): A Survey of Existing Systems and A Proposed Distributed Architecture" (hereinafter, "DIDS February 1991") does not contain greater disclosure than the references relating to DIDS that were cited to the Examiner and considered during prosecution of the patents-in-suit and thus is cumulative.

To the extent that the Defendants contend that the article L.T. Heberlein et al., "A Network Security Monitor," Proc. 1990 Symposium on Research in Security and Privacy, pp. 296-304, Oakland, CA, May 1990, and DIDS February 1991 or DIDS October 1991 are one reference for 102(b) purposes, this contention is improper. *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) (For an anticipatory

reference "[t]o incorporate material by reference, the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents.")

The '338 Patent

The Defendants have not shown that DIDS February 1991 or DIDS October 1991 anticipates the independent claims of the '338 patent. Specifically, they have not shown that either article discloses and/or enables building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, comparing such profiles, or determining whether the difference between them indicates suspicious activity as required by claims 1, 21, 24, and their dependent claims. Similarly, Defendants have not shown that DIDS February 1991 or DIDS October 1991 discloses and/or enables the at least one measure used to build the statistical profile monitoring data transfers, errors, or network connections, as required by claims 1, 24, and their dependent claims.

The dependent claims of the '338 patent include numerous additional limitations that the Defendants have not shown to be disclosed in the DIDS articles. For example, they have not shown that these articles disclose and/or enable the measure monitoring data transfers by monitoring network packet data transfer errors, monitoring data transfers by monitoring network packet data transfer errors, monitoring data transfers by monitoring network packet data transfer volume, monitoring network connections by monitoring network connection requests, monitoring network connections by monitoring network connection denials, monitoring network connections by monitoring a correlation of network connection requests and network connection denials, monitoring data transfers by monitoring error codes included in a network packet, monitoring error codes comprising a privilege error code, or monitoring error codes comprising an error code indicating a reason a packet was rejected, as required by claims 3-10, respectively.

Nor have Defendants shown that DIDS February 1991 or DIDS October 1991 discloses responding based on determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity, as required by claim 11, because, as discussed above, these articles do not disclose and/or enable such profiles. Similarly, the Defendants have not shown that these articles disclose and/or enable multiple short-term monitoring statistical profiles that comprise profiles that monitor different anonymous FTP sessions as required by claim 22 or deinterleaving packets to identify a short-term statistical profile as required by claim 23.

Further, Defendants have not shown that either DIDS February 1991 or DIDS October 1991 enables transmitting the event record to a network monitor that receives event records from multiple network monitors as required by claim 14 or that the network monitors include a network monitor that correlates activity in the multiple network monitors based on the received event records as required by claim 15. See, e.g., DIDS October 1991 at 175 (Conclusions) and 176 (Figs. 1-2); *Snapp Thesis* at 4 (Fig. 1), 6 (Fig. 2), 14 (Fig. 3), 5 ("The prototype environment consists of a single LAN segment with several hosts running. . ."), at 39 ("Long-term plans include. . . expanding the system to cover arbitrarily wide area networks"); *Mukherjee* 1994 at 36 ("Generalization of the monitored environment beyond the local area is an open problem."). Nor have Defendants shown that either DIDS article discloses altering analysis of the network packets as required by claim 16 or severing a communication channel as required by claim 17. Finally, they have not shown that DIDS February 1991 or DIDS October 1991 discloses receipt of packets by a network entity that comprises a gateway, router, or proxy server as required by claim 19.

The '203 and '615 Patents

The Defendants have not shown that DIDS February 1991 or DIDS October 1991 anticipates the independent claims of the '203 or '615 patents. Defendants have not shown that either article enables a method for use on an enterprise network, a plurality of network monitors, or integration of reports of suspicious activity from a plurality of network monitors by one or more hierarchical monitors as required by claims 1 and 12 of the '203 patent, claims 1 and 13 of the '615 patent, and their dependent claims. See, e.g., DIDS October 1991 at 175 (Conclusions) and 176 (Figs. 1-2); *Snapp Thesis* at 4 (Fig. 1), 6 (Fig. 2), 14 (Fig. 3), 5 ("The prototype environment consists of a single LAN segment with several hosts running. . ."), at 39 ("Long-term plans include. . . expanding the system to cover arbitrarily wide area networks"); *Mukherjee* 1994 at 36 ("Generalization of the monitored environment beyond the local area is an open problem.").

Furthermore, all claims of the '203 patent require network monitors that detect suspicious activity based on analysis of network traffic data selected from the following categories: network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet. Defendants have not shown that either DIDS article discloses and/or enables monitoring such network traffic. Similarly, all claims of the '615 patent require analysis of network traffic selected from the following: network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols. Defendants have not shown that either DIDS article discloses and/or enables monitoring such network traffic.

The dependent claims of the '203 and '615 patents include numerous additional limitations that the Defendants have not shown to be disclosed by the DIDS articles. For example, they have not shown that either DIDS February 1991 or DIDS October 1991

discloses correlating intrusion reports from a plurality of network monitors as required by claims 2 and 13 of the '203 patent and claims 2 and 14 of the '615 patent. Also, they have not shown that either DIDS article enables invoking countermeasures to a suspected attack as required by claims 3 and 14 of the '203 patent and claims 3 and 15 of the '615 patent. Further, they have not shown that either DIDS article discloses an API for encapsulation of monitor functions and integration of third-party tools as required by claims 4 and 15 of the '203 patent and claims 4 and 16 of the '615 patent. Nor have Defendants shown that either DIDS article discloses a network monitor deployed at a gateway, router, or proxy server as required by claims 6 and 17 of the '203 patent and claims 6 and 18 of the '615 patent.

Claims 8-10 and 18-21 of the '203 patent and claims 8-11 and 19-22 of the '615 patent require a plurality of service monitors, a domain monitor, or an enterprise monitor. Defendants have not shown that either DIDS article discloses and/or enables any of these features. See, e.g., DIDS October 1991 at 175 (Conclusions) and 176 (Figs. 1-2); *Snapp Thesis* at 4 (Fig. 1), 6 (Fig. 2), 14 (Fig. 3), 5 ("The prototype environment consists of a single LAN segment with several hosts running. . ."), at 39 ("Long-term plans include. . . expanding the system to cover arbitrarily wide area networks"); *Mukherjee* 1994 at 36 ("Generalization of the monitored environment beyond the local area is an open problem."). Nor have Defendants shown that either DIDS article enables the use of a statistical detection method as required by claim 7 of the '615 patent.

The '212 Patent

The Defendants have not shown that DIDS February 1991 or DIDS October 1991 anticipates any independent claim of the '212 patent. Claims 1, 14, and their dependent claims require use in an enterprise network, a plurality of network monitors, and a hierarchical monitor that automatically receives and integrates reports of suspicious activity from a plurality of network monitors. Defendants have not shown that either

DIDS article discloses any of these features. See, e.g., DIDS October 1991 at 175 (Conclusions) and 176 (Figs. 1-2); *Snapp Thesis* at 4 (Fig. 1), 6 (Fig. 2), 14 (Fig. 3), 5 ("The prototype environment consists of a single LAN segment with several hosts running. . ."), at 39 ("Long-term plans include. . . expanding the system to cover arbitrarily wide area networks"); *Mukherjee* 1994 at 36 ("Generalization of the monitored environment beyond the local area is an open problem."). Additionally, Defendants have not shown that either DIDS article enables a network monitor that utilizes a statistical detection method as required by claims 1, 14, and their dependent claims.

The dependent claims of the '212 patent includes numerous additional limitations that the Defendants have not shown to be disclosed by the DIDS articles. For example, Defendants have not shown that DIDS February 1991 or DIDS October 1991 discloses and/or enables a monitor that uses both signature matching and a statistical method as required by claim 3. Nor have they shown that either article enables correlation of intrusion reports from a plurality of network monitors as required by claims 4 and 15 or invoking countermeasures as required by claims 5 and 16. Further, the Defendants have not shown that either DIDS article discloses an API for encapsulation of monitor functions and integration of third-party tools as required by claims 6 and 17 or a network monitor that is deployed at a gateway, router, or proxy server, as required by claims 8 and 19.

Defendants have also not shown that either DIDS article discloses and/or enables a plurality of service monitors, a domain monitor, or an enterprise monitor as required by claims 9-12 and 20-23. See, e.g., DIDS October 1991 at 175 (Conclusions) and 176 (Figs. 1-2); *Snapp Thesis* at 4 (Fig. 1), 6 (Fig. 2), 14 (Fig. 3), 5 ("The prototype environment consists of a single LAN segment with several hosts running. . ."), at 39 ("Long-term plans include. . . expanding the system to cover arbitrarily wide area networks"); *Mukherjee* 1994 at 36 ("Generalization of the monitored environment beyond the local area is an open problem.").

10. ISM

Defendants have not shown that "Internetwork Security Monitor: An Intrusion-Detection System for Large-Scale Networks" (hereinafter, "ISM") anticipates and/or renders obvious in combination with DIDS October 1991 any claim of the patents-in-suit for at the least the following reasons:

Defendants' assertion that ISM and DIDS October 1991 constitute a single disclosure for purposes of 35 U.S.C. §102(b) is improper. *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) (For an anticipatory reference "[t]o incorporate material by reference, the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents.") Also, to the extent that the Defendants contend that the article L.T. Heberlein et al., "A Network Security Monitor," Proc. 1990 Symposium on Research in Security and Privacy, pp. 296-304, Oakland, CA, May 1990, and DIDS October 1991 is one reference for 102(b) purposes, this contention is also improper. See Id.

The '203 and '615 Patents

Defendants have not shown that ISM anticipates any independent claim of the '203 or '615 patents. All claims of the '203 patent require network monitors that detect suspicious activity based on analysis of network traffic data selected from the following categories: network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet. Defendants have not shown that ISM discloses and/or enables monitoring such network traffic. Similarly, all claims of the '615 patent require analysis of network traffic selected from the following: network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a

network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols. Defendants have not shown that ISM discloses and/or enables monitoring such network traffic.

Furthermore, all claims of the '203 and '615 patents require a hierarchical monitor automatically receiving and integrating the reports of suspicious activity from the network monitors. Defendants have not shown that ISM enables such a hierarchical monitor. ISM is merely "exploring the feasibility of different design alternatives." (ISM at 263). ISM's authors recognize that "[o]ther future work includes testing, refining, and extending the protocols described here. As we move from design and testing to full implementation, we will probably find flaws with our initial design." (Id. at 271). Another article authored by the same set of authors two years after ISM notes that "[g]eneralization of the monitored environment beyond the local area is an open problem" and characterizes ISM as "a preliminary design." B. Mukherjee et al., *Network Intrusion Detection*, IEEE Network, May-June 1994, Vol. 8, No. 3, at 33. For similar reasons, Defendants have not shown that ISM enables the additional limitations of dependent claims 7-11, 18-22 of the '203 patent and claims 8-12 and 19-23 of the '615 patent. Further they have not shown that ISM discloses correlating intrusion reports reflecting underlying commonalities, as required by claims 2 and 13 of the '203 patent and claims 2 and 14 of the '615 patent, nor that it discloses invoking countermeasures to a suspected attack, as required by claims 3 and 14 of the '203 patent and claims 3 and 15 of the '615 patent. Also, Defendants have not shown that ISM discloses an API for encapsulation of monitor functions and integration of third party tools as required by claims 4 and 15 of the '203 patent and claims 4 and 16 of the '615 patent.

Defendants inconsistently assert that ISM discloses network monitors being deployed at a gateway, router, or proxy server as required by claims 6 and 17 of the '203 patent and claims 6 and 18 of the '615 patent. These inconsistencies reinforce the fact that, Defendants have not shown that ISM discloses network monitors being deployed at

a gateway, router, or proxy server, as opposed to disclosing an ISM monitor that monitors all traffic in and out of a site. (ISM at 270).

For the reasons discussed above with respect to DIDS and ISM, Defendants have failed to show that alone or in combination these references disclose and/or enable every limitation of any claim of the '203 or '615 patents. For this reason, ISM in combination with DIDS does not render any claim of the '203 or '615 patents obvious.

The '212 Patent

Defendants have not shown that ISM anticipates any independent claim of the '212 patent. Defendants have not shown that ISM discloses and/or enables monitors using a statistical detection method as required by all claims of the '212 patent. All claims of the '212 patent also require a hierarchical monitor automatically receiving and integrating the reports of suspicious activity from network monitors. As discussed above with respect to the '203 and '615 patents, Defendants have not shown that ISM enables such a hierarchical monitor. For similar reasons, they have also not shown that ISM enables the additional limitations of dependent claims 8-13 and 19-24.

Nor have Defendants shown that ISM discloses and/or enables the use of a monitor that uses a signature matching detection method with or without statistical detection methods as required by claims 2 and 3. The Defendants have not shown that ISM discloses correlating intrusion reports reflecting underlying commonalities as required by claims 4 and 15, nor have they shown that ISM discloses invoking countermeasures to a suspected attack as required by claims 5 and 16. Lastly, Defendants have not shown that ISM discloses an API for encapsulation of monitor functions and integration of third party tools as required by claims 6 and 17.

Defendants inconsistently assert that ISM discloses network monitors being deployed at a gateway, router, or proxy server as required by claims 8 and 19. Defendants' inconsistency reinforces, that, in fact, they have not shown that ISM

discloses a network monitor being deployed at a gateway, router, or proxy server as opposed to an ISM monitor that monitors all traffic in and out of a site. (ISM at 270).

For the reasons discussed above with respect to DIDS and ISM, Defendants have failed to show that alone or in combination these references disclose and/or enable every limitation of any claim of the '212 patent. For this reason, ISM in combination with DIDS does not render any claim of the '212 patent obvious.

The '338 Patent

Defendants do not assert that ISM alone anticipates any claim of the '338 patent, rather Defendants assert that ISM in combination with DIDS renders the '338 claims obvious.

For the reasons discussed above, Defendants have failed to show that DIDS teaches several of the limitations of the '338 claims. Defendants also fail to show that ISM discloses and/or enables these missing limitations. Defendants have not shown that ISM discloses and/or enables building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, comparing such profiles, or determining whether the difference between them indicates suspicious activity as required by independent claims 1, 21, and 24. Similarly, Defendants have not shown that ISM discloses and/or enables the at least one measure used to build the statistical profile monitoring data transfers, errors, or network connections, as required by independent claims 1 and 24.

With respect to the dependent claims of the '338 patent, Defendants do not even allege that ISM discloses the numerous additional limitations of claims 2-10, 16, 17, 19, and 22. They do not show that ISM discloses responding based on determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity, as required by claim 11, because, as discussed above, ISM does not disclose and/or enable such profiles. Similarly, the

Defendants have not shown that ISM discloses and/or enables deinterleaving packets to identify a short-term statistical profile as required by claim 23.

Further, as discussed above with respect to the '203 and '615 patents, Defendants have not shown that ISM enables transmitting the event record to a network monitor that receives event records from multiple network monitors as required by claim 14 or that the network monitors include a network monitor that correlates activity in the multiple network monitors based on the received event records as required by claim 15.

Thus Defendants have failed to show that alone or in combination ISM and DIDS disclose and/or enable every limitation of any claim of the '338 patent. For this reason, ISM in combination with DIDS does not render any claim of the '338 patent obvious.

11. GRIDS

The GrIDS (1996) article is not an enabling reference for any of the subject matter it is alleged to invalidate. The Defendants also have not provided evidence to establish that the article they refer to as GrIDS 1997 is a printed publications within the meaning of 35 U.S.C.§ 102(b) before November 9, 1997.

'203 and '615 patents

GrIDS does not disclose any of the claims of the '203 or '615 patents. The Graph Engine in GrIDS creates graphs based on activities within a certain portion of a network. ("GrIDS 1997" 16). The Graph Engine uses "Rulesets" to determine when to create graphs and what information should be included in the graph. ("GrIDS 1997" 11). The Rulesets also determine when the graphs indicate suspicious activity and then create alerts and reports associated with the graphs that are sent to the Graph Engine log file. ("GrIDS 1997" 14, 22). The citations by the Defendants show that although there is a hierarchy of Graph Engines, the higher level engines in the GrIDS system do not perform the required tasks of the hierarchical monitors recited in independent claims 1 and 12 of the '203 patent and claims 1 and 13 of the '615 patent. The only time information is sent

to a higher level engine occurs when a Graph Engine sends a subset of the information in a graph to a higher level engine, and this information is only sent when a connection is made to a computer outside its portion of the network. ("GrIDS 1997" 16). Therefore, the citations by the Defendants show that the higher level engines do not automatically receive and integrate reports of suspicious activity as recited in claims 1 and 12 of the '203 patent and claims 1 and 13 of the '615 patent. The Graph Engines at the lower levels of the hierarchy use their Rulesets to analyze the graphs they have built. They then create alerts and reports based on this analysis. ("GrIDS 1997" 20-22). However, rather than sending these reports to the higher level monitors, they are sent to that Graph Engine's log file. ("GrIDS 1997" 22).

Further, because the higher level monitors do not receive reports of suspicious activities, they do not correlate the reports as recited in dependant claims 2 and 13 of the '203 patent and claims 2 and 14 of the '615 patent, nor can the integrating of reports comprise invoking countermeasures as recited in by dependent claims 3 and 14 of the '203 patent and claims 3 and 15 of the '615 patent. Further, the Defendants' citations do not disclose that the monitors are deployed at gateways, routers, proxy servers as recited in dependent claims 6 and 17 of the '203 patent and dependent claims 6 and 18 of the '615 patent.

12. NETRANGER

Defendants have not shown that NetRanger User Guide 1.3.1 or the NetRanger product anticipates any claim of the '203 or '615 patents for at the least the following reasons.

Several documents relating to NetRanger were cited to the Examiner during prosecution of the '615 patent, including, Cisco Secure Intrusion Detection System, Release 2.1.1, NetRanger User's Guide, Version 2.1.1., © 1998, Cisco Systems, Inc., allegedly released on Apr. 1998; Cisco Secure Intrusion Detection System 2.1.1 Release Notes for NetRanger 2.1.1, © 1999-2002, Cisco Systems, Inc.; Hartley, B., "Intrusion

Detection Systems: What You Need to Know," Business Security Advisor Magazine, Doc # 05257, allegedly dated Sep. 1998; Hurwicz, M., "Cracker Tracking: Tighter Security with Intrusion Detection," BYTE.com, allegedly dated May 1998; R. Power, et al., "CSI Intrusion Detection System Resource," allegedly dated July 1998. As the Examiner initialed the IDS listing these references he is presumed to have considered them in his decision to issue the patent. Further, his decision to issue the patent over those references later after the patent's priority date is presumed correct.

The Defendants have not shown that NetRanger User Guide 1.3.1 was a publication prior to November 9, 1997. Similarly, the Defendants have not shown that the materials they rely on to demonstrate the capabilities of the NetRanger product describe a product that was publicly available prior to November 9, 1997. The *SQL queries* and the *NetRanger Training Slides* are undated. *Performance and Security Test* is dated April 30, 1997, however it is labeled "FOR OFFICIAL USE ONLY" and indicates that distribution is "limited to U.S. Government Agencies Only." Furthermore, the Defendants have not shown that these materials all relate to the same product. Similar issues exist with respect to the additional documents that Defendants identify as related to NetRanger.

The '203 and '615 Patents

Defendants have not shown that either NetRanger User Guide 1.3.1 or the NetRanger product disclose automatic integration of reports of suspicious activity from a plurality of network monitors by a hierarchical monitor as required by claims 1 and 12 of the '203 patent, claims 1 and 13 of the '615 patent, and their dependent claims.

The dependent claims of the '203 and '615 patents include numerous additional limitations that the Defendants have not shown to be disclosed by NetRanger. For example, Defendants have not shown that either NetRanger User Guide 1.3.1 or the NetRanger product discloses correlating intrusion reports reflecting underlying

commonalities as required by claims 2 and 13 of the '203 patent and claims 2 and 14 of the '615 patent. Nor have Defendants shown that NetRanger User Guide 1.3.1 or the NetRanger product discloses an API for encapsulation of monitor functions and integration of third-party tools as required by claims 4 and 15 of the '203 patent and claims 4 and 16 of the '615 patent. Additionally, they have not shown that NetRanger User Guide 1.3.1 or the NetRanger product discloses network monitors deployed at a gateway, router, or proxy server, facilities on the enterprise network as required by claims 6 and 17 of the '203 patent and claims 6 and 18 of the '615 patent.

13. REALSECURE

The Defendants have not shown that RealSecure anticipates any claim of the '203 or '615 patents for at the least the following reasons:

Several documents describing early versions of RealSecure were cited to the Examiner during the prosecution of the '615 patent, including, for example, Hartley, B., "Intrusion Detection Systems: What You Need to Know," Business Security Advisor Magazine, Doc # 05257, allegedly dated Sep. 1998; Hurwicz, M., "Cracker Tracking: Tighter Security with Intrusion Detection," BYTE.com, allegedly dated May 1998; R. Power, et al., "CSI Intrusion Detection System Resource," allegedly dated July 1998; and Internet Security Systems, "Intrusion Detection for the Millennium," ISS Technology Brief, Date Unknown. As the Examiner initialed the IDS listing these reference he is presumed to have considered them in his decision to issue the patent. Further, his decision to issue the patent over these references is presumed correct.

The Defendants rely on several RealSecure User Guides and Reference Manuals with copyright dates 1996-1997. The Defendants have not shown that these guides and manuals were publicly available or when. Defendants also rely on a document referred to as "*RealSecure Release Dates Table.*" (ISS 358384; SYM_P_0504850). There is no indication of the source of this document and the document does not specify the meaning

of the listed dates. Finally, several of the additional references cited by Defendants, including *Real-Time Attack Recognition and Response: A Solution for Tightening Network Security*, are improperly characterized as 102(b) references as the Defendants have not shown that these references were publicly available more than a year before the priority date of the '203 and '615 patents.

The '203 and '615 Patents

Defendants have not shown that the RealSecure product version or its associated documentation allegedly available before the critical dates discloses a hierarchical monitor that *automatically integrates* reports of suspicious activity as required by all the independent claims of the '203 and '615 patents. All RealSecure's Administrator's Module does is list attack events according to their assigned priority. It does not automatically integrate or correlate attack events.

The dependent claims of the '203 and '615 patents include numerous additional limitations that the Defendants have not shown to be disclosed by the asserted early version of RealSecure. For example, Defendants have not shown that the early version of RealSecure relied upon discloses automatically correlating intrusion reports as required by claims 2 and 13 of the '203 patent and claims 2 and 14 of the '615 patent. As discussed above, RealSecure's Administrator's Module merely lists attack events. Its generation of "meaningful reports from its event log files" (*Real-Time Attack Recognition and Response: A Solution for Tightening Network Security* at 11) does not occur automatically; it requires administrator involvement. (See e.g., *RealSecure 1.1. User Guide and Reference Manual* at Chapter 5.)

Also, Defendants have not shown that the asserted reference discloses an API for encapsulation of monitor functions and integration of third-party tools as required by claims 4 and 15 of the '203 patent and claims 4 and 16 of the '615 patent. Rather RealSecure discloses the potential use of a third party decision support system. (July 21,

1997 *FAQ* at Q29). Additionally, Defendants have not shown disclosure of a network monitor deployed at a gateway, router, or proxy server as required by claims 6 and 17 of the '203 patent and claims 6 and 18 of the '615 patent. Nor have Defendants shown that the asserted reference discloses a plurality of domain monitors or an enterprise monitor as required to anticipate claims 9, 10, 20, or 21 of the '203 patent or claims 10, 11, 21, or 22 of the '615 patent.

14. NETWORK FLIGHT RECORDER

The Network Flight Recorder ("NFR") paper, when taken alone or in combination with the "NIDES", "Ji-Nao", "Ji-Nao Slides", "EMERALD", or Real Secure 1.1 User's Guide fails to anticipate or render obvious any claims of the '338, '203, '615 or '212 patents.

First, it would not be obvious to combine the NFR paper with any of the "NIDES", "Ji-Nao", "Ji-Nao Slides", "EMERALD", or Real Secure 1.1 User's Guide references simply because all of the references allegedly relate to network-based intrusion detection analysis. That fact, even if true, merely satisfies one prong of the test for whether the references can be combined to render the claimed inventions obvious. To satisfy the second prong of the test, the Defendants must show that there is a suggestion or motivation to combine the references. The Defendants have failed to do this, and have therefore failed to meet their burden of proof that any combination of references they cite renders the claimed inventions obvious.

The '212 Patent

Defendants have failed to show that the NFR paper anticipates or renders obvious claims 1-24 of the '212 patent for at least the following reasons.

The NFR paper fails to disclose deploying a plurality of network monitors to detect suspicious network activity by analyzing network traffic data. Instead, the paper

discloses deploying one or more network packet suckers, which do little more than gather network packet data. (NFR at 2). The data is then passed from the packet suckers to a decision engine "using a generalized API intended to allow packet suckers to be separate processes from the engine." Id. Thus, the disclosure of one or more packet suckers is not a disclosure of one or more decision engines or network monitors that detect suspicious network activity based on the analysis of network traffic data.

Second, all of the claims of the '212 patent recite that at least one of the network monitors detects suspicious network activity using a statistical detection method. While the NFR paper discloses generating alerts in response to satisfying certain so-called "N-code" filters, it fails to disclose any specific N-code filters, and in particular any N-code filters that use statistical detection methods to generate alerts. The Defendants rely on a passage indicating that NFR's decision engine "keeps statistics pertaining to variance in the delivery of packets" to satisfy this limitation of the '212 patent's claims. However, the very next line of the NFR paper indicates that "[t]hese statistics are used to determine when the engine will stop watching a given connection," rather than to determine suspicious network activity. (Id. at. 2).

Finally, all of the claims of the '212 patent also recite automatically receiving and integrating reports of suspicious activity in one or more hierarchical network monitors. The Defendants rely on the NFR paper's disclosure of a "query backend" to meet this limitation. But the so-called "query backend" is not a network monitor since it does not receive and analyze network packet data. Nor is it a hierarchical network monitor that automatically receives and integrates reports of suspicious network activity from other network monitors. Instead, the "query backend" is a duplicate copy of the NFR decision engine's backend recorder. It was developed to allow a network administrator to query the data in a decision engine's backend using SQL commands without actually having to query the decision engine itself. It therefore avoids disrupting the flow of network traffic data into the decision engine. (See id. at 3-4) Thus, the "query backend" is not a

network monitor, and does not automatically receive and integrate reports of suspicious network activity.

The NFR paper fails to anticipate claims 2 and 3 of the '212 patent for the same reason it fails to anticipate claim 1. Claim 2 requires at least one of the network monitors in the plurality of network monitors recited in claim 1 to detect suspicious network activity using a signature matching detection method. Claim 3 further requires the at least one network monitor of claim 2 to detect suspicious network activity using a statistical detection method in addition to its signature matching detection method. Yet, as discussed above, the NFR paper fails to disclose specific "N-code" filters that are run to generate alerts, and whether these N-code filters use statistical, signature-based, or some other intrusion detection method to generate alerts.

The NFR paper fails to anticipate claims 4, 5, 15 and 16 of the '212 patent as well. These claims recite network monitoring systems and methods that include hierarchical monitors that integrate reports of suspicious network activity by correlating intrusion reports reflecting underlying commonalities (claims 4 and 15), and that invoke countermeasures to suspected attacks (claims 5 and 16). The Defendants rely on certain features of the query-backend such as the fact that it has a CGI interface, can be accessed with SQL commands, and includes GUI elements called "packages" that are designed to simplify the user's view of the data that is stored in the backend to meet these limitations. They also rely on the fact that alerts that are generated by the decision engine, which is separate from the query-backend, can be sent via a number of delivery routes such as to an email address, a facsimile number, or a print queue. However, as explained above, the query backend is little more than a database of information. It is not a hierarchical monitor, and it does not automatically integrate reports of suspicious network activity. It therefore cannot correlate the reports it has not automatically received and integrated (claims 4 and 15), and cannot invoke countermeasures in response to suspected attacks (claims 5 and 16).

The NFR paper fails to anticipate claims 6 and 17 of the '212 patent, which require the plurality of network monitors recited in claims 1 and 14, respectively, to include an API for encapsulation of monitor functions and integration of third-party tools. To meet this limitation, the Defendants rely on the NFR paper's disclosure that its packet suckers pass network header information to its decision engine using "a generalized API intended to allow packet suckers to be separate processes from the engine." (p. 2). As discussed above, NFR's packet suckers do not do network analysis and are therefore not network monitors. While they may have APIs, their APIs do not encapsulate network monitor functions as claimed, but instead allow the packet suckers "to be separate processes from the [decision] engine." Id. .

The NFR paper fails to render obvious claims 8-13 and 19-24 of the '212 patent. The Defendants rely on the combination of the NFR paper with the RealSecure 1.1 User's Guide, the NIDES reference, and the EMERALD reference, to meet the specific limitations recited in these claims. However, the Defendants have provided no motivation to combine the NFR paper with either one or more of the RealSecure 1.1 User's Guide, the NIDES reference, or the EMERALD reference. Therefore, the Defendants have failed to establish that claims 8-13 and 19-24 are obvious in view of these combinations.

The '203 and '615 Patents

The NFR paper is cited as anticipating or rendering obvious claims 1-6 and 8-22 of the '203 patent and claims 1-23 of the '615 patent. Much of the Defendants' analysis of particular limitations in the '203 and '615 claims is duplicative of their analysis of similar limitations in the '212 claims. Therefore, the NFR paper fails to anticipate or render obvious the claims of the '203 and '615 patent for the same reasons the NFR paper fails to anticipate or render obvious the claims of the '212 patent. These include the following.

Like the claims of the '212 patent, the independent claims of the '203 and '615 patents recite systems and methods of monitoring an enterprise network by deploying a plurality of network monitors in the enterprise network, and using the network monitors to detect suspicious network activity based on the analysis of network traffic data. As with the '212 patent, the Defendants rely on the disclosure of one or more network packet suckers in the NFR paper to read on this limitation. However, the NFR paper discloses that the network packet suckers do little more than gather and forward network data. (NFR at 2). They do not analyze that data for any reason, let alone to detect suspicious network activity.

Similarly, like the claims of the '212 patent, all of the claims of the '203 and '615 patents recite automatically receiving and integrating reports of suspicious activity in one or more hierarchical network monitors. As with the '212 patent, the Defendants rely on the NFR paper's disclosure of a "query backend" to meet this limitation. But as discussed above, the "query backend" is neither a network monitor that analyzes network packet data, nor a hierarchical monitor that automatically receives and integrates reports of suspicious network activity from other network monitors.

Finally, all of the claims of the '203 and '615 patents recite that the network monitors detect suspicious network activity by analyzing certain types of network traffic data, including network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, and error codes included in a network packet. The NFR paper fails to disclose this limitation. While the NFR paper discloses generating alerts in response to satisfying certain so-called "N-code" filters, it fails to disclose any specific N-code filters that generate alerts, and in particular, it fails to disclose alert-generating N-code filters that analyze the types of network traffic data that are recited in the claims of the '203 patent.

The NFR paper fails to anticipate claims 2, 3, 13 and 14 of the '203 and '615 patents for the same reason it fails to anticipate claims 4, 5, 15 and 16 of the '212 patent.

Specifically, these claims recite network monitoring systems and methods that include hierarchical monitors that integrate reports of suspicious network activity by correlating intrusion reports reflecting underlying commonalities (claims 2 and 13), and that invoke countermeasures to suspected attacks (claims 3 and 14). The Defendants rely on the same features of the query-backend and alert delivery routes available to NFR's decision engine to argue the NFR paper anticipates these claims. However, as explained above, NFR's query backend and decision engine are not hierarchical monitors, do not automatically integrate reports of suspicious network activity, and therefore cannot correlate such reports (claims 2 and 13), and invoke countermeasures in response to suspected attacks (claims 3 and 14).

The NFR paper fails to anticipate claims 4 and 15 of the '203 patent and claim 4 and 16 of the '615 patent for the same reason it fails to anticipate claims 6 and 17 of the '212 patent. Specifically, these claims recite that the plurality of network monitors recited in the independent claims include an API for encapsulation of network monitor functions and integration of third-party tools. The NFR paper's disclosure that its packet suckers pass network header information to its decision engine using "a generalized API intended to allow packet suckers to be separate processes from the engine," (NFR at 2), fails to meet this limitation for the same reasons it fails to meet the same limitation in claims 6 and 17 of the '212 patent.

The NFR paper similarly fails to render obvious claims 6 and 17 of the '203 patent and claims 6 and 18 of the '615 patent. The Defendants rely on the combination of the NFR paper with the RealSecure 1.1 User's Guide, the NIDES reference, and the EMERALD reference, to meet the specific limitations recited in these claims. However, the Defendants have provided no motivation to combine the NFR paper with either one or more of the RealSecure 1.1 User's Guide, the NIDES reference, or the EMERALD reference. Therefore, the Defendants have failed to establish that these claims are obvious in view of these combinations.

The '338 Patent

The NFR paper is also cited as rendering obvious claims 1-27 of the '338 patent. In particular, the Defendants assert that the claims of the '338 patent are obvious in view of the combination of the NFR paper with either the "EMERALD", the "Ji-Nao", or the "Jou" papers. As before, however, the Defendants have failed to provide any motivation for combining the NFR paper with either the "EMERALD", "Ji-Nao", or "Jou" papers. Therefore, the Defendants have failed to meet their burden to establish that any claims of the '338 patent are obvious. Moreover, the Defendants have failed to establish the obviousness of any claims of the '338 patent for the following reasons.

First, all of the claims of the '338 patent require building at least one short-term and at least one long-term statistical profile of at least one measure of network packets that monitors data transfers, errors or network connections. The Defendants rely on the NFR paper's disclosure of a "histogram" backend to satisfy this limitation. But NFR's disclosure of its "histogram" backend is neither a disclosure of a short-term nor a long-term statistical profile of a network packet measure as required by the claims. The NFR paper describes its "histogram" backend as a "columnar table of data, either totaling discrete values in the columns or incrementing them." (NFR at 3). In footnote 3, the NFR paper admits the "histogram" backend has been unconventionally named, and that it "should have [been] called [a] spreadsheet" to avoid confusion. Storing event records in a spreadsheet, even multiple event records, does not disclose building at least one short-term and at least one long-term statistical profile of a network packet measure.

Moreover, the NFR paper in combination with any of the references cited fails to render any of the claims of the '338 patent obvious by failing to disclose building statistical profiles from any of the particular network packet measures recited in the claims. The Defendants rely on the NFR paper's disclosures to support their obviousness arguments regarding the type of network packet measures to monitor via statistical profiles. But the NFR paper fails to specifically disclose or to even suggest statistically

monitoring any measure of data transfers, errors or network connections (claims 1-20, 21-23 and 24), including packet data transfer commands (claim 2), packet data transfer errors (claim 3), packet data transfer volume (claim 4), connection requests (claim 5), connection denials (claim 6), a correlation of connection requests and denials (claim 7), network packet error codes (claim 8), including privilege error codes (claim 9) and error codes indicating why a packet was rejected (claim 10). Thus, the NFR paper in combination with any of the other references cited fails to render obvious any of claims 1-24.

The NFR paper in combination with any of the references cited fails to render obvious any of the '338 claims by failing to disclose comparing at least one long-term and at least one short-term statistical profile. The Defendants rely on the NIDES and the Ji-Nao papers to disclose this limitation. However, there is no motivation to combine the NFR paper with the NIDES or Ji-Nao papers. As explained above, the NFR paper fails to disclose building short-term or long-term statistical profiles of any network measure. Thus, there is no motivation to combine the NFR paper with the NIDES or Ji-Nao paper or any other paper that may disclose comparing long-term and short-term statistical profiles.

The NFR paper in combination with any of the references cited also fails to render claims 12-15 obvious because the combination fails to disclose transmitting an event record to a "network monitor" (claim12), and in particular to a "hierarchically higher" network monitor (claim 13) that receives event records from multiple network monitors (claim 14) and correlates them (claim 15). The Defendants rely on the EMERALD paper to disclose each of these limitations, however, there is no motivation to combine the NFR paper with the EMERALD paper. As explained above, the NFR paper fails to disclose deploying a plurality of network monitors in an enterprise network. Thus, there is no motivation to combine the NFR paper with the EMERALD paper or any other paper that may disclose transmitting event records from one network monitor to another network

monitor (claim 12) that exists at hierarchically higher level in the network (claim 13), or that receive "alerts" from multiple network monitors (claim 14) and "correlates" them (claim 15). For at least these reasons, the NFR paper cannot be combined with any of the cited references to render claims 12-15 obvious.

The NFR paper in combination with any of the references cited also fails to render claim 16 obvious because it fails to disclose altering the analysis of network packets in response to determining suspicious network activity. The Defendants rely on the NFR paper's disclosures to support their obviousness arguments regarding this limitation, but the NFR paper fails to specifically disclose or to even suggest altering the analysis of network packets in response to determining suspicious network activity. Certainly the paper's disclosure of a "histogram" backend, fails to disclose or even suggest altering the analysis of network packet data in response to determining suspicious network activity as the Defendants contend. As explained above, the NFR paper's "histogram" backend is nothing more than a spreadsheet of historical network traffic data. It neither analyzes, nor alters the analysis of network packet data. Consequently, the Defendants have failed to establish that claim 16 is obvious in view of the combination of the NFR paper with any of the other references cited by the Defendants.

The combination of the NFR paper and any of the references relied on by Defendants also fails to render claims 21-23 obvious, which require building a long-term and multiple short-term statistical profiles (claim 21), where the short-term profiles monitor different anonymous FTP sessions (claim 22), and are built by de-interleaving packet data (claim 23). As noted above, the NFR paper does not specifically disclose building either short-term or long-term statistical profiles, let alone building multiple short-term statistical profiles. Consequently, there is no motivation to combine it with the Ji-Nao reference relied on by Defendants, or any other reference that may disclose building long-term and short-term statistical profiles. For these reasons, the NFR paper in combination with any of the cited references fails to render claims 21-23 obvious.

Claim 24 recites a computer product including instructions for performing the method recited in claim 1. Thus, the combination of the NFR paper with any of the cited references fails to render claim 24 obvious for the same reasons any such combination fails to render claim 1 obvious. Claims 25-27 recite receiving packets at a virtual private network entity. The Defendants rely on the same arguments they applied to claim 1 to argue that the NFR paper in combination with one or more of the cited references renders claims 25-27 obvious, however, since the combination of the NFR paper with the cited references did not render claim 1 obvious for the reasons noted above, the combination of the NFR paper with the cited references does not render claims 25-27 obvious for at least the same reasons.

15. NETSTALKER WITH HP OPENVIEW

The Defendants have not established that NetStalker and HP OpenView were combined to constitute prior art under 35 U.S.C. § 102 (b) prior art. *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) (For an anticipatory reference "[t]o incorporate material by reference, the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents."). Further the HP OpenView and the Internet standards documents to not constitute one reference that can be combined for 35 U.S.C. § 102 (b). Id. Additionally, the asserted combination of NetStalker with the references that Defendants cited do not establish obviousness under 35 U.S.C. § 103 because Defendants fail to establish that there would be a motivation to combine any of them.

The '203 and '615 Patents

The Defendants' citations to the NetStalker reference fail to anticipate any of the claims of the '203 or '615 patents. First, NetStalker does not have hierarchical monitors nor perform hierarchical event monitoring as required by claim 1 and claim 12 of the

'203 patent and claim 1 and claim 13 of the '615 patent. Rather, routers send event data, i.e. "instances of system calls or services by system utilities that are recorded in the audit trail" (GL-2) to the Misuse Detector at the NetStalker server where it is analyzed. The Misuse Detector analyzes the data to determine if it matches signatures. (6-1, 6-2, 6-15). The Misuse Detector will then create an alert or report and/or log the data. (6-15, 6-18). However, there is no hierarchical monitor that automatically receives and integrates this data as recited in independent claims 1 and 12 of the '203 patent and claims 1 and 13 of the '615 patent. Instead, the Log Manager in NetStalker organizes the data in various locations such as local drives, tape drives or remote archived storage, based solely on file age and current disk capacity. (7-2).

For these reasons, Defendants' citations to the NetStalker reference also fail to show anticipation of any of the dependent claims of the '203 and '615 patents. Defendants' citations to NetStalker fail to disclose correlation of intrusion reports, as recited in claims 2 and 13 of the '203 patent and claims 2 and 14 of the '615 patent. Further, because there is no integration of the intrusion reports, the integrating cannot comprise invoking counter measures as required by claims 3 and 14 of the '203 patent and claims 3 and 15 of the '615 patent

Further, the routers disclosed in NetStalker do not monitor data, they simply send events to the NetStalker. (6-2). Therefore, it is the NetStalker servers that receive information from routers. To the extent NetStalker discloses anything that could be described as a "network monitor" that monitor is not located at a gateway, router or proxy server as required by claims 6 and 17 of the '203 patent and claims 6 and 18 of the '615 patent.

16. HP OPENVIEW

The HP OpenView and Internet Standards documents cited by Defendants do not constitute one reference that can be combined for 35 U.S.C. § 102 (b). *Advanced*

Display Sys., Inc. v. Kent State Univ., 212 F.3d 1272, 1282 (Fed. Cir. 2000) (For an anticipatory reference "[t]o incorporate material by reference, the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents.") Additionally, the Defendants have not established obviousness under 35 U.S.C. § 103 for HP OpenView and the other references cited because they have provided no evidence even addressing, let alone clearly and convincingly establishing, a motivation to combine those references.

The '203 and '615 Patents

HP OpenView by itself or in combination with the Internet Standards does not anticipate any of the claims of the '203 or '615 patents. HP OpenView simply discloses a platform for managing networks. It provides a standard graphic interface so that multiple network applications can share a common display and alarm system and provides basic network management functions to interface with devices on the network. ISS26778. The Defendants' citations to the HP OpenView and Internet Standards do not disclose network intrusion detection as required by every claim of the '203 and '615 patents. Further, the Defendants' citations to HP OpenView do not disclose detecting suspicious network activity based on analysis of network traffic data selected from network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, or error codes included in a network packet as required by independent claims 1 and 12 of the '203 patent and 1 and 13 of the '615 patent. While the Internet Standards may disclose using "managed objects" to manage a network and that those objects can include such things as number of packets received via the interface which were discarded because of an unknown or unsupported protocol, they do not disclose using this data to detect suspicious network activity. Further, the Defendants' citations to the HP OpenView and the Internet Standards do not disclose using the network traffic data listed above to detect

network activity by using one or more hierarchical monitors, nor are there hierarchical monitors that receive and integrate reports of suspicious activity as required by independent claims 1 and 12 of the '203 patent and 1 and 13 of the '615 patent. Additionally, there are no reports of suspicious activity as recited in claims 1 and 12 of the '203 patent and claims 1 and 13 of the '615 patent disclosed in Defendants' citations.

Finally, the Defendants' citations do not disclose correlating reports nor invoking countermeasure as part of integrating the reports as required by dependant claims 2, 3, 13 and 14 of the '203 patent and claims 2, 3, 14 and 15 of the '615 patent.

17. NETWORK LEVEL INTRUSION DETECTION

Defendants have failed to show that the paper entitled "The Architecture of a Network Level Intrusion Detection System," (ANLIDS), anticipates any of the claims of the '338 patent under 102(b) for at least the following reasons.

All claims of the '338 patent recite building at least one short-term and one long-term statistical profile from at least one measure of network packets, comparing the short-term and long-term statistical profiles, and determining whether the difference between the short and long-term statistical profiles is indicative of suspicious network activity. The ANLIDS paper fails to disclose any of these limitations. While the paper advertises that the ANLIDS system is "based on a statistical characterization of network behavior," p. 3, it actually describes a rules-based method for determining suspicious network activity. For example, the paper discloses using "a classifier system and genetic algorithm which learns normal patterns of network traffic and flags deviations from those patterns." (p. 4). The classifier system is described as "a parallel, message-passing, rule-based system," (p. 12), that is "essentially a system to generate and test hypothesis." (p. 15). The classifier system is never described as a statistically based system that uses long and short-term statistical profiles. Thus, rather than disclosing a statistical method for determining suspicious network activity, the ANLIDS paper discloses a rules-based

method for determining suspicious network activity. Consequently, the ANLIDS paper fails to anticipate any of the claims of the '338 patent for at least this reason.

Moreover, the ANLIDS paper fails to anticipate the claims of the '338 patent by failing to disclose building or comparing statistical profiles from the network packet measures that are recited in the claims, namely, data transfers, errors, or network connections. For example, the ANLIDS paper discloses that there are only four values of a network packet that are "important to the classifier system. These are the packet size value, the time-stamp value, and the Ethernet source-destination ordered pair." (p.9). Thus, the ANLIDS paper fails to specifically disclose building and comparing statistical profiles that monitor data transfers, errors or network connections (claims 1, 24 and 25), packet data transfer commands (claim 2), packet data transfer errors (claim 3), packet data transfer volume (claim 4), connection requests (claim 5), connection denials (claim 6), a correlation of connection requests and denials (claim 7), network packet error codes (claim 8), including privilege error codes (claim 9) and error codes indicating why a packet was rejected (claim 10). The ANLIDS paper therefore fails to anticipate these claims for at least this reason.

The ANLIDS paper also fails to anticipate claim 16, which requires altering analysis of the network packets in response to determining suspicious network activity. The ANLIDS paper fails to disclose altering the analysis of network packets. In fact, the paper does not disclose responding to suspected network intrusions at all. At most, the paper suggests that future work on the program will involve "developing appropriate reactions to detected intrusions . . . . [that] may include delaying or ignoring communications involving the suspected participating nodes." (ANLIDS at 17). There is no disclosure that in addition to ignoring nodes participating in suspicious network activity, the ANLIDS program would in any way alter its analysis of network data. For these reasons, the ANLIDS paper fails to anticipate claim 16.

The ANLIDS paper also fails to anticipate claims 21-23, which require building a long-term and multiple short-term statistical profiles (claim 21), where the short-term profiles monitor different anonymous FTP sessions (claim 22), and are built by de-interleaving packet data (claim 23). As noted above, the ANLIDS paper does not specifically disclose building or using short-term statistical profiles, let alone building multiple short-term statistical profiles. Instead, it discloses detecting suspicious network activity using a rules-based classifier system. Moreover, the ANLIDS paper specifically states that there are only four pieces of network packet data "which are important to the classifier system. These are the packet size value, the time-stamp value, and the Ethernet source-destination ordered pair." (ANLIDS at 9). ANLIDS thus fails to disclose building or using a statistical profile to monitor anonymous FTP sessions, or the need to de-interleave network packets for the purpose of building multiple short-term statistical profiles. For these reasons, the ANLIDS paper fails to anticipate claims 21-23.

The ANLIDS paper fails to anticipate claim 24 for the same reasons it fails to anticipate claim 1. Claims 25-27 recite receiving packets at a virtual private network entity. The ANLIDS paper only discloses receiving network traffic on an Ethernet network, and fails to disclose that the packets are received by a virtual private network entity.

In addition to the foregoing, the ANLIDS paper does not anticipate any claims of the '338 patent because it is non-enabling. For example, on pages 10 and 11 the paper discloses a number of event categories that *may* be useful to detect network intruders. The paper goes on to say, however, that "[p]roper choice of meaningful categories . . . is a difficult task. The difficulty lies in the fact that patterns of normal network behavior will not be apparent unless good classification of event categories are chosen. A good category, however, is by definition one which reveals patterns of normal behavior." (ANLIDS at 11). As a result of this uncertainty, the paper indicates in its summary that the focus of the author's research "is to determine the *feasibility* of network level

monitoring to protect network resources from attack." (Id. at 17)(emphasis added). The authors admit that their goal, rather than their accomplishment, is "to build an off-line prototype system capable of learning normal patterns of network use and flagging departures from those patterns of normality. Such a system will *permit verification of the hypothesis* that intrusive attacks are in fact detectable as deviations from a rule-based profile of normal behavior." (Id. 17)(emphasis added). Thus, not only did the authors of ANLIDS not know which rules would work to detect network intrusions, they did not know that their system as a whole would work for that purpose. Thus, the ANLIDS paper is not an enabling disclosure.

18. '750 THOMPSON

The Defendants have not shown that U.S. Patent No. 5,825,750 ("the '750 patent") anticipates any claim of the '338 patent. The '750 patent purports to describe a system and method for detecting abnormal use of an ATM network by maintaining a user profile associated with a node in the network and analyzing deviation from the profile. See, Col. 2, lines 9-19.

With regard to the independent claims, there is no disclosure or suggestion in the '750 patent of building a long-term statistical profile. Instead, the '750 patent refers to gathering historical information about network use (Col. 4, lines 54-67) and employing a dynamic programmable threshold representing the limit of expected behavior (Col. 5, lines 27-38). Moreover, the system of the '750 patent does not build a short-term statistical profile. Rather, it compares every requested transmission to the historical data to determine whether there is a deviation. See, Col. 5, lines 14-26.

The dependent claims of the '338 patent include numerous limitations not disclosed or suggested by the '750 patent. For example, there is no indication that the system of the '750 patent monitors network packet data transfer commands, network packet data transfer volume, connection requests, connection denials, correlation of

connection requests with denials, network packet data transfer errors, or error codes as required by claims 2-8 and 10. Additionally, there is no disclosure or suggestion of transmitting reports to hierarchically higher network monitors that do correlation as required by claims 13-15. There is no disclosure or suggestion of altering analysis of network packets or severing a communication channel as required by claims 16 and 17 respectively. The '750 patent does not refer to deploying monitors at a gateway, router or proxy server as required by claim 19.

19. FAULT DETECTION IN AN ETHERNET NETWORK VIA ANOMALY DETECTORS (THE "FEATHER REFERENCE")

The Defendants have not shown that the Feather reference anticipates any claim of the '338 patent.

With regard to the independent claims, the Feather reference includes no disclosure or suggestion of building a short-term statistical profile. Rather, the Feather reference looks for single events that fall outside some statistically determined threshold. See, e.g., graphs on ISS_00348306-00348307; SYM_P_0501826-0501827. Additionally, the Feather reference only discloses looking at data packet frequency. See, e.g., graphs on ISS_00348306-00348307; SYM_P_0501825-0501827. This activity does not amount to building statistical profiles based on at least one measure monitoring data transfers, errors or network connections as required by the claims.

The dependent claims of the '338 patent include numerous limitations not disclosed or suggested by the Feather reference. For example, there is no indication that the system of the Feather reference monitors network packet data transfer commands, network packet data transfer volume, connection requests, connection denials, correlation of connection requests with denials, network packet data transfer errors, or error codes as required by claims 2-8 and 10. Additionally, there is no disclosure or suggestion of transmitting reports to hierarchically higher network monitors that do correlation as

required by claims 13-15. There is no disclosure or suggestion of altering analysis of network packets or severing a communication channel as required by claims 16 and 17 respectively. The Feather reference does not refer to deploying monitors at a gateway, router or proxy server as required by claim 19.

20. STAKE OUT NETWORK SURVEILLANCE

The Defendants have not shown that the "Stake Out Network Surveillance" white paper ("Stake Out") anticipates any claim of the '338 patent under 102(b) for at least the following reasons.

All of the claims of the '338 patent require building at least one short-term and at least one long-term statistical profile of at least one measure of network packets that monitors data transfers, errors or network connections. The Stake Out paper fails to anticipate any claim of the '338 patent because it fails to specifically disclose building or comparing at least one short-term and one long-term statistical profile from at least one recited measure of the network packets that are received. At most, the paper discloses that certain network characteristics are "learned over time . . . and retained in a database," (Stake Out at 6), and that "artificial intelligence techniques [are used] to compare network traffic against what the surveillance system has learned as normal behavior." (Id. at 7). Such a disclosure fails to specifically identify *how* network characteristics are learned, how they are stored in a database, and how network traffic is compared to learned normal behavior. In particular, it fails to disclose that any of these tasks are or can be performed by building and comparing short-term and long-term statistical profiles as required by all of the claims. Therefore, the Stake Out paper fails to anticipate the claims for at least this reason.

Moreover, the Stake Out paper fails to anticipate any of the claims of the '338 patent by failing to disclose building or comparing statistical profiles from any of the particular network packet measures that are recited in the claims. For example, the only

"network traffic characteristics" that are specifically identified by the Stake Out paper as being "measurably predictable" are "time of day, number and types of packets, [and] common destination / source address combinations." (Id. at 6-7). The paper fails to specifically disclose statistically comparing (via short and long-term statistical profiles or any other method) any measure of data transfers, errors or network connections (claim 1, 21 and 24), such as packet data transfer commands (claim 2), packet data transfer errors (claim 3), packet data transfer volume (claim 4), connection requests (claim 5), connection denials (claim 6), a correlation of connection requests and denials (claim 7), network packet error codes (claim 8), including privilege error codes (claim 9) and error codes indicating why a packet was rejected (claim 10). Thus, the Stake Out paper fails to anticipate any claim of the '338 patent for at least this reason as well.

The Stake Out paper also fails to anticipate claims 12-15 because it fails to disclose transmitting an event record to a "network monitor" (claim 12), and in particular to a "hierarchically higher" network monitor (claim 13) that receives event records from multiple network monitors (claim 14) and correlates them (claim 15). The Stake Out paper fails to disclose such a system of transmitting and sharing event records by and between "network monitors." At most, the Stake Out paper discloses sending "alerts" to one or more centrally monitored network management systems. (Id. at 8). There is no disclosure that the one or centrally monitored systems are themselves network monitors (claim 12), that exist at hierarchically higher levels in the network (claim 13), or that receive "alerts" from multiple network monitors (claim 14) and "correlate" them (claim 15). For at least these reasons, the Stake Out paper fails to anticipate claims 12-15.

The Stake Out paper also fails to anticipate claim 16, which requires altering analysis of the network packets in response to determining suspicious network activity. At most, the paper discloses initiating a *duplicate* listening process to capture packet data from an attacking host when suspicious activity has been detected. (Id. at 9). This duplicate listening process is part of an Evidence Logging component that does little

more than log suspicious event data for the purpose of preserving evidence. Id. There is no disclosure that the event data that is logged by this duplicate listening process is ever analyzed, let alone analyzed by an altered analysis process. Moreover, there is no disclosure that Stake Out's continuing analysis of incoming network packet data is in any way altered based on the determination of suspicious network activity. For these reasons, the Stake Out paper fails to anticipate claim 16.

The Stake Out paper also fails to anticipate claim 17, which requires severing a communication channel upon detecting suspicious network activity. On page 2, in a section on "Background," the Stake Out paper discloses that "[s]imilar technologies for network monitoring and security have generally been limited to detection and notification capabilities. More sophisticated systems . . . further provide denial of access upon detection of recognizable unauthorized activities." (Id. at 2). When read in context, this section does not indicate that Stake Out or a more sophisticated version of Stake Out provides a denial of access response. Rather, it indicates that more sophisticated versions of "similar technologies," which are not named in the paper, provide denial of access response. For at least this reason, the Stake Out paper fails to anticipate claim 17.

The Stake Out paper also fails to anticipate claims 21-23, which require building a long-term and multiple short-term statistical profiles (claim 21), where the short-term profiles monitor different anonymous FTP sessions (claim 22), and are built by de-interleaving packet data (claim 23). As noted above, the Stake Out paper does not specifically disclose building either short-term or long-term statistical profiles, let alone building multiple short-term statistical profiles. At most it discloses that certain network characteristics can be "learned over time . . and retained in a database," and that artificial intelligence can be used "to compare network traffic against what the surveillance system has learned as normal behavior." (Stake Out at 6-7). Assuming *arguendo* that this passage *does* disclose building and comparing short-term and long-term statistical profiles (which SRI denies), it does not disclose building multiple short-term statistical

profiles for comparison to a long-term statistical profile. Moreover, the only network characteristics Stake Out specifically discloses as being "measurably predictable" indicators of normal network behavior are "time of day, number and types of packets, [and] common destination / source address combinations." Id. Stake Out fails to disclose building a singe statistical profile to monitor anonymous FTP sessions, let alone multiple short-term statistical profiles, or the need to de-interleave network packets to build the multiple profiles. For these reasons, Stake Out fails to anticipate claims 21-23.

Claim 24 recites a computer product including instructions for performing the method recited in claim 1. Stake Out fails to anticipate claim 24 for the same reasons it fails to anticipate claim 1. Claims 25-27 recite receiving packets at a virtual private network entity. Stake Out only discloses receiving network traffic on an Ethernet network, and fails to disclose that the packets are received by a virtual private network entity.

21. EMERALD 1997, INTRUSIVE ACTIVITY 1991, NIDES 1994

Defendants' assertion that EMERALD 1997, Intrusive Activity 1991 and NIDES 1994 constitute a single disclosure for purposes of 35 U.S.C. §102(b) is improper. *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000). Further, as explained above, NIDES and EMERALD are not enabling references for the claims of the patents-in-suit. Intrusive Activity 1991 simply discloses the concept of reviewing network packets, rather than audit logs which does not enable the claims of the patents-in-suit either alone or in combination with the other asserted references. Therefore, Defendants' combination does not enable and/or render obvious any of the claims of the patents-in-suit.

22. AIS

The Defendants have not shown that the AIS reference anticipates any claim of any of the patents-in-suit. As an initial matter, the AIS reference is not an enabling disclosure. Rather, it is an extremely vague and high level description of what appears to be a hypothetical system. With regard to the independent claims of the '203 and '615 patents, the AIS reference is silent on the types of network traffic analyzed, which are required by the independent claims of the '203 and '615 patents.

23. DEFENDANTS' SUMMARY CHART

Defendants attempt to set forth an assertion that the patents-in-suit are obvious in light of the numerous references listed in Exhibit 23 to their invalidity contentions. Defendants, however, fail to show any combination that renders any claim of the patents-in-suit obvious. Defendants' attempt to create an obviousness argument based on the combination of so many unrelated references is improper and fails to disclose any particular contention in a manner sufficient for SRI to respond.

Nonetheless, SRI incorporates its discussion of the specific references addressed above and notes that the Defendants have failed to identify any motivation to combine any particular combination of the tens of references identified in Exhibit 23.

35 U.S.C. §112 CONTENTIONS

Defendants' contention that the claims-at-issue are invalid for failure to satisfy the best mode requirement under 35 U.S.C. § 112 is based solely on speculation. The Defendants have failed to identify any evidence that the inventors did not provide the U.S. Patent Office with the most complete source code they believed was available to them as of November 9, 1998. Defendants fail to disclose any other particular contention regarding other basis for invalidity under 35 U.S.C. § 112 in a manner sufficient for SRI to respond.

INTERROGATORY NO. 9 (SIC - 20):

State, in as much detail as possible, SRI's contentions as to why the facts disclosed in ISS's Supplemental Response to SRI's Interrogatory No. 11 and in the Answers of ISS-GA and ISS-DE do not render the patents-in-suit unenforceable by SRI's inequitable conduct. Your answer should include: (1) a statement as to whether or not you contend that the inventors and/or their agents made each identified misrepresentation or omission of fact; (b) for each misrepresentation or omission of fact, a statement as to whether or not you contend that the inventors and/or their agents acted with intent; and for each publication identified, a detailed explanation of why the publication is not material, or an admission that the publication is material.

RESPONSE TO INTERROGATORY NO. 9 (SIC - 20):

SRI objects to this interrogatory as premature. Claim construction has not yet occurred in this matter. SRI objects to this interrogatory as seeking information protected from disclosure by the attorney-client privilege and/or attorney work product doctrines. Discovery and analysis in this case are ongoing. Any response by SRI is preliminary and SRI reserves the right to supplement its response as discovery and analysis proceed.

Without waiving any specific and any applicable general objection, SRI responds as follows:

SRI incorporates by reference Plaintiff and Counter-Defendant SRI International, Inc.'s Answers to Counterclaims of Defendants.

At no time and with respect to no reference did SRI, its attorneys, or the named inventors intend to deceive the patent office by withholding references. During the prosecution of the patents-in-suit, SRI cited literally dozens of prior art references, which indicates SRI's good faith effort to place as much prior art at the disposal of the Examiner as possible.

With regard to the IDES and "network" NIDES publications, these references are not material or alternatively are cumulative of other art before the Examiner. As set forth above with regard to the invalidity contentions, vague, non-enabled references relating to applying IDES or NIDES on a network are not material. To the extent that the IDES and NIDES references contain material information, SRI cited numerous references related to IDES and NIDES including, for example, Jarvis et al., "The NIDES Statistical Component Description and Justification", March 7, 1994, which was cited in the applications that resulted in the patents-in-suit. SRI also cited numerous articles authored by Dorothy Denning and Teresa Lunt relating to the technology of NIDES and IDES. To the extent that publications related to any of SRI's systems, including IDES, NIDES and EMERALD are material, these references are cumulative of, at least, Porras et al., "Monitoring Enabling Responses to Anomalous Live Disturbances", October 9, 1997.

With regard to the Ji-Nao reference or the Ji-Nao slides, ISS presents no evidence that these publications are prior art to the patents-in-suit or that SRI, its attorneys or the named inventors were aware of them. ISS only indicates that SRI was aware of the Ji-Nao system. Moreover, as set forth above with regard to the invalidity contentions, the Ji-Nao reference is immaterial because it does not anticipate or render obvious the patents-in-suit. Additionally, the Ji-Nao reference is cumulative of many other pieces of prior art including the numerous references to IDES and NIDES that were before the Examiner. Finally, the Ji-Nao reference is at least cumulative of Porras et al., "Monitoring Enabling Responses to Anomalous Live Disturbances", October 9, 1997.

With regard to the "NSM" reference, as set forth above, this reference is not material as it does not anticipate or render obvious any claim of the '338 patent. Moreover, this reference is cumulative at least of the various IDES and NIDES related references before the Examiner. Additionally, this reference is cumulative at least of Snapp et al., "DIDS (Distributed Intrusion Detection System) – Motivation, Architecture,

and An Early Prototype" since DIDS, on information and belief, incorporates the technology disclosed in the NSM reference.

Dated: December 15, 2005

FISH & RICHARDSON P.C.

By: _____
Timothy Devlin (#4241)
John F. Horvath (#4557)
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Gina M. Steele (CA Bar No. 233379)
Katherine D. Prescott (CA Bar No. 215496)
Michael J. Curley (CA Bar No. 230343)
FISH & RICHARDSON P.C.
500 Arguello Street, Suite 500
Redwood City, California 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff
SRI INTERNATIONAL, INC.

50315424.doc